SOURCE: 72 FR 18758, Apr. 13, 2007, unless otherwise noted.

Subpart A—DoD Policy

§310.1 Reissuance.

This part consolidates into a single location (32 CFR part 310) Department of Defense (DoD) policies and procedures for implementing the Privacy Act of 1974, as amended (5 U.S.C. 552a) by authorizing the development, publication and maintenance of the DoD Privacy Program set forth by DoD Directive 5400.11[1] and 5400.11–R,[2] both entitled: ''DoD Privacy Program.''

§310.2 Purpose.

This part:

(a) Updates the established policies and assigned responsibilities of the DoD Privacy Program pursuant to 5 U.S.C. 552a (also known and referred to in this part as ''The Privacy Act'') and Office of Management and Budget (OMB) Circular No. A–130.

(b) Authorizes the Defense Privacy Board and the Defense Data Integrity Board.

(c) Prescribes uniform procedures for implementation of and compliance with the DoD Privacy Program.

(d) Delegates authorities and responsibilities for the effective administration of the DoD Privacy Program.

[80 FR 4207, Jan. 27, 2015]

§310.3 Applicability and scope.

(a) This part applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this part as the ''DoD Components'').

(b) For the purposes of subsection (i), ''Criminal penalties,'' of The Privacy Act, any DoD contractor and any employee of such a contractor will be considered to be an employee of DoD when DoD provides by a contract for the operation by or on behalf of DoD of a system of records to accomplish a DoD function. DoD will, consistent with its authority, cause the requirements of section (m) of The Privacy Act to be applied to such systems.

[80 FR 4207, Jan. 27, 2015]

§310.4 Definitions.

The following definitions apply to this part:

Access. The review of a record or a copy of a record or parts thereof in a system of records by any individual.

Agency. For the purposes of disclosing records subject to the Privacy Act among the DoD Components, the Department of Defense is considered a single agency. For all other purposes to include requests for access and amendment, denial of access or amendment, appeals from denials, and record keeping as relating to release of records to non-DoD Agencies, each DoD Component is considered an agency within the meaning of the Privacy Act.

Breach. A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information (PII), whether physical or electronic.

Computer matching. The computerized comparison of two or more automated systems of records or a system of records with non-federal records. Manual comparisons are not covered.

Confidential source. A person or organization who has furnished information to the Federal Government under an express promise, if made on or after September 27, 1975, that the person's or the organization's identity shall be held in confidence or under an implied promise of such confidentiality if this implied promise was made on or before September 26, 1975.

Disclosure. The information sharing or transfer of any PII from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, government agency, or private entity other than the subject of the

[1] Copies may be obtained at *http://www.dtic.mil/whs/directives.*

[2] See footnote 1 to §310.1.

record, the subject's designated agent, or the subject's legal guardian.

DoD contractor. Any individual or other legal entity that:

(1) Directly or indirectly (*e.g.*, through an affiliate) submits offers for or is awarded, or reasonably may be expected to submit offers for or be awarded, a government contract, including a contract for carriage under government or commercial bills of lading, or a subcontract under a government contract; or

(2) Conducts business, or reasonably may be expected to conduct business, with the federal government as an agent or representative of another contractor.

DoD personnel. Service members and federal civilian employees.

Federal benefit program. A program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals.

Federal personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits).

Individual. A living person who is a U.S. citizen or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual also may act on behalf of an individual, except as otherwise provided in this part. Members of the Military Services are ''individuals.'' Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not ''individuals'' when acting in an entrepreneurial capacity with the DoD, but persons employed by such organizations or entities are ''individuals'' when acting in a personal capacity (*e.g.*, security clearances, entitlement to DoD privileges or benefits).

Individual access. Access to information pertaining to the individual by the individual or his or her designated agent or legal guardian.

Information sharing environment. Defined in Public Law 108–458, ''The Intelligence Reform and Terrorism Prevention Act of 2004''.

Lost, stolen, or compromised information. Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purpose where one or more individuals will be adversely affected. Such incidents also are known as breaches.

Maintain. The collection, maintenance, use, or dissemination of records contained in a system of records.

Member of the public. Any individual or party acting in a private capacity to include Federal employees or military personnel.

Mixed system of records. Any system of records that contains information about individuals as defined by the Privacy Act and non-U.S. citizens and/or aliens not lawfully admitted for permanent residence.

Non-Federal agency. Any state or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a computer matching program.

Official use. Within the context of this part, this term is used when officials and employees of a DoD Component have a demonstrated a need for the record or the information contained therein in the performance of their official duties, subject to DoD 5200.1–R.[3]

Personally identifiable information (PII). Information used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, home phone numbers, other demographic, personnel, medical, and financial information. PII includes any information that is linked or linkable to a specified individual, alone, or when combined with other personal or identifying information. For purposes of this part, the

[3] See footnote 1 to § 310.1

term PII also includes personal information and information in identifiable form.

Privacy Act request. A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual. These records must be maintained in a system of records.

Protected health information (PHI). Defined in DoD 6025.18–R, ''DoD Health Information Privacy Regulation'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/602518r.pdf*).

Recipient agency. Any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a computer matching program.

Record. Any item, collection, or grouping of information in any media (*e.g.*, paper, electronic), about an individual that is maintained by a DoD Component, including, but not limited to, education, financial transactions, medical history, criminal or employment history, and that contains the name, or identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, a voice print, or a photograph.

Risk assessment. An analysis considering information sensitivity, vulnerabilities, and cost in safeguarding personal information processed or stored in the facility or activity.

Routine use. The disclosure of a record outside the Department of Defense for a use that is compatible with the purpose for which the information was collected and maintained by the Department of Defense. The routine use must be included in the published system notice for the system of records involved.

Source agency. Any agency which discloses records contained in a system of records to be used in a computer matching program, or any state or local government, or agency thereof, which discloses records to be used in a computer matching program.

Statistical record. A record maintained only for statistical research or reporting purposes and not used in whole or in part in making determinations about specific individuals.

System of records. A group of records under the control of a DoD Component from which PII is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular uniquely assigned to an individual.

System of records notice (SORN). A notice published in the FEDERAL REGISTER that constitutes official notification to the public of the existence of a system of records.

[80 FR 4207, Jan. 27, 2015]

§ 310.5 Policy.

It is DoD policy that:

(a) An individual's privacy is a fundamental legal right that must be respected and protected.

(1) The DoD's need to collect, use, maintain, or disseminate (also known and referred to in this part as ''maintain'') PII about individuals for purposes of discharging its statutory responsibilities will be balanced against their right to be protected against unwarranted privacy invasions.

(2) The DoD protects individuals' rights, consistent with federal laws, regulations, and policies, when maintaining their PII.

(3) DoD personnel and DoD contractors have an affirmative responsibility to protect an individual's privacy when maintaining his or her PII.

(4) Consistent with section 1016(d) of Public Law 108–458 and section 1 of Executive Order 13388, ''Further Strengthening the Sharing of Terrorism Information to Protect Americans'', the DoD will protect information privacy and provide other protections relating to civil liberties and legal rights in the development and use of the information sharing environment.

(b) The DoD establishes rules of conduct for DoD personnel and DoD contractors involved in the design, development, operation, or maintenance of any system of records. DoD personnel and DoD contractors will be trained with respect to such rules and the requirements of this section and any other rules and procedures adopted pursuant to this section and the penalties for noncompliance. The DoD Rules of Conduct are established in § 310.8.